ABSTRACT

A method of verifying a transaction over a data communication system between a first and second correspondent through the use of a certifying authority. The certifying authority has control of a certificate's validity, which is used by at least the first correspondent. The method comprises the following steps. One of the first and second correspondents advising the certifying authority that the certificate is to be validated. The certifying authority verifies the validity of the certificate attributed to the first correspondent. The certifying authority generates implicit signature components including specific authorization information. At least one of the implicit signature components is forwarded to the first correspondent for permitting the first correspondent to generate an ephemeral private key. At least one of the implicit signature components is forwarded to the second correspondent for permitting recovery of an ephemeral public key corresponding to the ephemeral private key. The first correspondent signs a message with the ephemeral private key and forwards the message to the second correspondent. The second correspondent attempts to verify the signature using the ephemeral public key and proceeds with the transaction upon verification.